Ottomi-Ops 3.0 智能运维平台产品白皮书

产品名称：Ottomi-Ops 3.0 智能运维平台

文档版本：V3.0

编制单位：上海奥腾计算机科技有限公司

日期：2026 年 6 月

目 录

第一章 产品概述

1.1 产品定位

Ottomi-Ops 3.0 是一款面向单租户独立部署场景的智能运维与数据安全一体化平台。平台具备无 Agent（Agentless）监控采集与智能告警等基础运维能力，并重点提供数据库备份与恢复、数据安全监测两大核心能力，形成集监控告警、数据安全、备份恢复于一体的综合运维解决方案。

平台定位为公共数据运营平台等关键数据基础设施的**"数字哨兵"与"黑匣子"**——既通过实时监控保障业务连续性（哨兵），又通过数据库安全审计与备份恢复保障数据资产的机密性、完整性与可追溯性（黑匣子），满足国家数据安全法及行业监管的刚性要求。

1.2 核心价值

开箱即用：无 Agent 部署，监控类型 YAML 定义驱动，快速覆盖主流中间件与主机

数据安全闭环：监控告警+数据库审计+防火墙阻断+备份恢复，形成完整安全防线

国产化适配：原生支持达梦、金仓数据库备份恢复，适配信创环境

生产级可靠：备份双副本、恢复二次确认、命令参数化执行、密码脱敏等安全设计

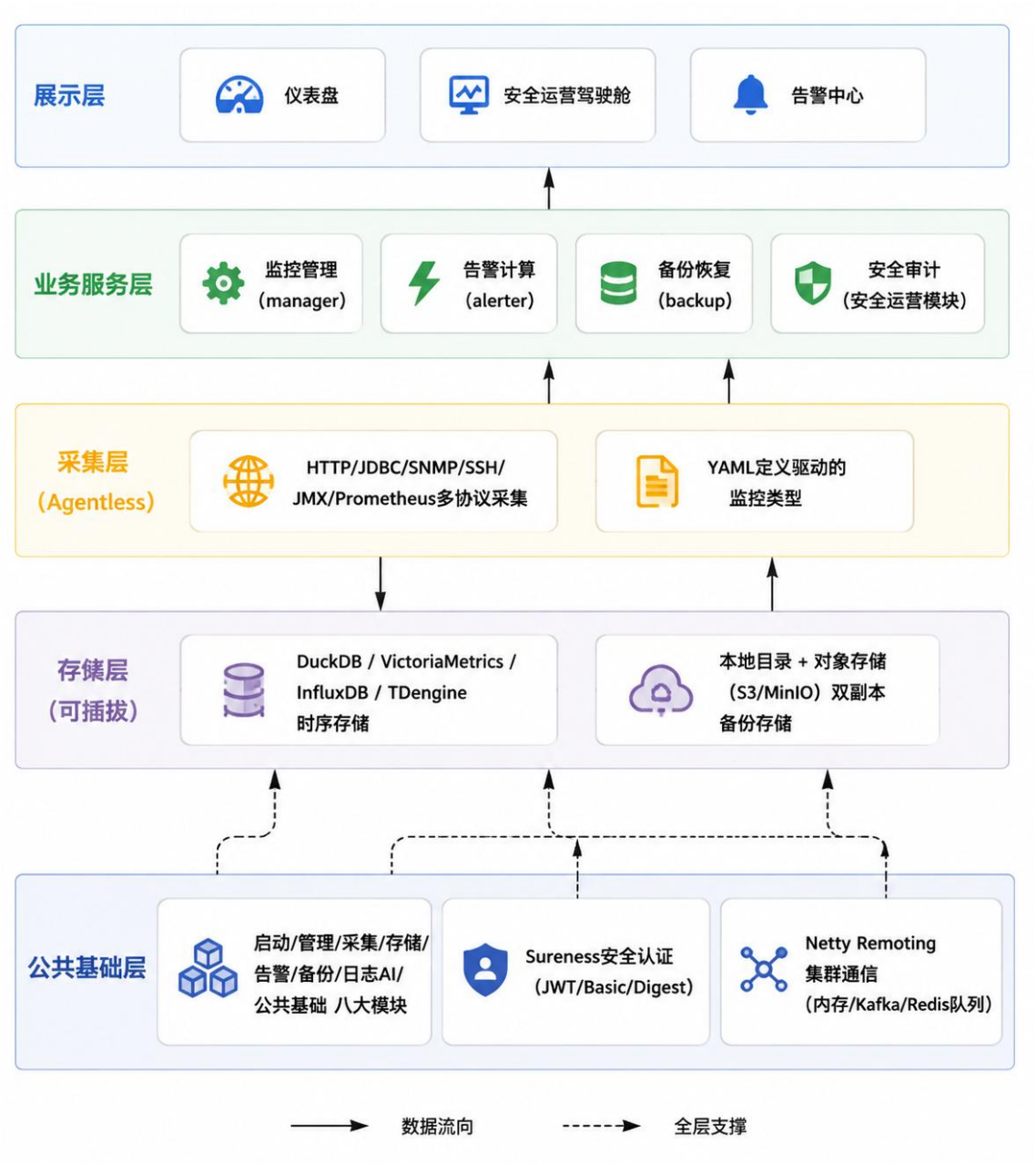
交付灵活：功能裁剪层支持按客户场景定制交付形态

1.3 产品能力边界

Ottomi-Ops 3.0 与数据中台产品（Ottomi-Nexus 3.0）协同工作、职责分明：**Nexus 负责数据治理与开发侧能力**（编目、归集、治理、开发、资产、服务、合约），**Ops 负责运维安全侧能力**（全栈监控、智能告警、备份恢复、数据安全监测）。两者同底座部署、统一告警联动——Nexus 识别"什么数据敏感"，Ops 监控"谁在碰数据"，协同形成完整安全闭环。

第二章 产品架构

2.1 总体架构



2.2 技术架构

层次	技术选型
后端语言	Java 25（JDK 25+）
后端框架	Spring Boot 4.0.3（Maven 多模块工程）
数据访问	Spring Data JPA + Flyway，支持 H2/MySQL/PostgreSQL
安全认证	Sureness + JWT/Basic/Digest
时序存储	DuckDB、VictoriaMetrics、InfluxDB、TDengine 等（可平滑切换）
集群通信	Netty Remoting，支持内存/Kafka/Redis 队列
前端框架	Angular 17.3 + TypeScript

层次	技术选型
前端 UI	ng-zorro-antd、ng-alain、@delon
可视化	ECharts + ngx-echarts
编辑器	Monaco Editor、ngx-markdown

后端模块组成：

模块	职责说明
startup（启动模块）	主启动包，组装所有后端模块，承载启动配置、数据库、认证与静态资源挂载
manager（管理模块）	核心管理 API：监控对象、采集调度、监控定义、插件等管理中枢
collector（采集模块）	采集系统，含 HTTP/JDBC/SNMP/SSH/JMX/Prometheus 等协议采集
warehouse（存储模块）	指标实时/历史存储与查询，适配多时序数据库后端
alerter（告警模块）	告警计算、收敛、静默、抑制与通知
backup（备份模块）	备份与恢复能力
log/ai（日志与 AI 模块）	日志中心、AI 能力（交付版可裁剪）
common（公共基础模块）	公共模型、工具、JPA 实体、配置、队列等

第三章 核心能力

3.1 基础设施监控

平台提供无 Agent（Agentless）的全栈监控能力，**无需在目标机器安装任何 Agent**，即可通过多种协议采集指标，大幅降低部署与运维成本。

- **多协议采集**：HTTP、JDBC、SNMP、SSH、JMX、Prometheus 等多种采集协议
- **监控定义驱动**：MySQL、Redis、Linux、Kubernetes、Prometheus 等大量内置监控类型，由 YAML 定义驱动，可快速扩展新资源类型
- **监控分类**：服务监控、程序监控、数据库监控、缓存监控、操作系统、中间件、大数据、Web 服务、云原生、网络设备、服务器、自定义监控十二类
- **指标存储**：采集指标实时入库，历史趋势可查，支持多时序数据库后端平滑切换
- **仪表盘**：监控大屏可视化呈现主机与服务的健康状态、实时指标与趋势

3.2 智能告警中心

告警系统覆盖告警全生命周期，从阈值计算到通知触达，确保安全事件分钟级响应。

- **告警规则**：指标阈值、日志关键字、表达式告警等多维告警规则
- **多渠道通知**：支持邮件、企业微信机器人等多种通知渠道精准推送
- **告警生命周期**：告警触发、确认、恢复全流程留痕，便于溯源
- **告警管理**：支持告警收敛、静默、抑制，避免告警风暴

3.3 备份与恢复

平台内置独立的备份恢复模块，为关键业务配置数据提供防丢失与可恢复能力：

能力	说明

能力	说明
备份通道	支持 MySQL（mysqldump/mysqlbinlog）、达梦数据库（dexp/dimp）、金仓数据库（sys_dump/sys_restore、sys_basebackup）——国产数据库备份恢复原生支持
备份模式	"定期全量+高频增量"组合备份；增量自动依赖全量基线，无基线时自动降级为全量，保证备份链完整
定时调度	基于 Cron 表达式的定时自动备份，支持启用/停用
双重存储	本地专用目录+对象存储（S3/MinIO 兼容协议）双副本，物理隔离规避单点故障
保留策略	按保留数量自动清理过期备份文件与记录，存储可控
数据恢复	支持恢复到新库，或覆盖原库（强制二次确认）；支持时间点还原
安全防护	ProcessBuilder 参数化命令执行、数据库名/路径白名单校验、密码不入日志、执行超时控制

备份功能菜单包括：**备份源**（配置备份目标连接信息，自动检测官方命令行工具可用性）、**备份策略**（配置备份目标、全量/增量方式、Cron 表达式、保留数量与存储目标）、**备份记录**（查看任务执行状态、文件大小、耗时与错误信息，支持手动触发）、**恢复任务**（选择备份记录执行恢复，覆盖原库需二次确认）。

3.4 数据安全监测

数据安全监测是平台面向"数据为中心的全链路安全防御"提供的核心增值能力，覆盖基础设施层、数据库层与计算任务层：

- **基础设施安全基座监测**：通过 SSH 协议定时执行安全检查命令，采集 SSH 暴力破解、sudo 提权、异常登录、关键文件完整性、异常进程等指标
- **数据库核心资产审计**：通过 JDBC 采集各数据库原生审计信息，构建用户权限、活跃会话、密码安全、权限变更、高危配置、DDL 变更等统一审计模型（覆盖 MySQL/PostgreSQL/Oracle/SQL Server）
- **数据库防火墙**：内置 SQL 注入特征库与高危操作规则（如无 WHERE 批量删除/更新、全表扫描、GRANT ALL、DROP/TRUNCATE 等），实时识别高危 SQL 会话并支持一键阻断（Kill）
- **数据计算任务合规追踪**：对接 DolphinScheduler/SeaTunnel 元数据库，对数据开发任务、批处理作业进行全流程安全跟踪
- **安全运营驾驶舱**：统一安全大屏汇聚主机入侵威胁、数据库安全评分、告警趋势等核心指标，提供全局态势决策视图

3.5 数据库安全网关（安全运营模块）

本模块面向核心数据服务的访问安全合规需求，提供一套覆盖**身份识别、访问控制、行为检测、实时阻断**的完整数据库安全防护体系。系统通过客户端 IP、客户端主机名、数据库账号、操作系统用户名、客户端工具等多个维度对用户身份进行综合识别，对进出核心数据服务的访问流量进行访问控制；依据预设的安全规则，实时识别各种可疑、违规的访问行为，对相应的 SQL 请求与会话执行实时放行或阻断。

七项核心能力：

能力	说明
敏感数据扫描	内置 10 类敏感数据规则（身份证/银行卡/手机号/护照号/车牌号/MAC 地址/港澳台通行证/邮箱判高危可终止会话，日期/时间判警告仅提示），支持自定义检测正则；内置规则可切换启用、可调整风险等级
攻击特征规则	内置 7 类攻击特征库：缓冲区溢出、SQL 注入、提权、高危 DDL、数据外泄、命令执行、系统表访问；运行中的 SQL 命中攻击特征即实时阻断；支持自定义攻击类型与检测正则
多数据源筛选管控	数据库实例下拉框自由切换目标数据源，每个数据源独立执行 SQL 审计、会话分析、风险识别与规则匹配
访问频次检测	规则要素：统计维度（同一会话/客户端 IP/数据库账号/客户端工具）+时间窗口（秒）+阈值（次数）+风险等级，超阈值即触发管控
自定义防护策略	支持按账号、数据库名、客户端工具、操作系统用户名、客户端 IP、操作类型、SQL 关键字 7 个维度制定精细化防护策略，每个维度支持精确等于/包含/正则匹配三种匹配方式
风险告警查询	查询条件支持账号/数据库名/客户端工具/操作系统用户名/客户端 IP/命令类型/会话 ID/SQL 关键字等字段；结果以会话列表呈现（会话 ID、用户、来源主机、数据库、客户端工具、OS 用户名、命令、运行时长、状态、SQL 文本、风险等级、风险原因），按高危/警告/正常分级统计与高亮显示，高危会话可直接终止
分组管理	安全规则按"敏感数据扫描/攻击特征/访问频次/防护策略"四大策略组归类管理，各组独立配置、独立生效；组内以"内置/自定义"标签区分，内置规则不可删除、自定义规则可完整维护

风险等级与处置策略：

风险等级	含义	处置
高危（DANGEROUS）	命中个人敏感信息/攻击特征/超频访问/防护策略等高危规则	进入实时阻断，支持终止会话
警告（WARNING）	命中日期、时间等弱敏感规则	可见提示，不可终止
正常（NORMAL）	未命中任何规则	正常放行

典型应用场景：

敏感数据防泄漏：业务人员执行含身份证号、银行卡号、手机号的查询时，会话自动标记高危并可终止，防止敏感数据批量外泄

SQL 注入防护：攻击者构造联合查询注入语句时，命中 SQL 注入攻击特征，会话被实时阻断

暴力访问管控：同一客户端 IP 在时间窗口内高频访问时，触发访问频次规则，自动提示/阻断

越权操作防护：非授权账号对生产库执行 DELETE、DROP 等操作时，命中防护策略规则，实时告警并可终止

3.6 功能菜单总览

菜单域	功能说明
概览	平台首页可视化大屏：主机与服务健康状态、实时指标趋势、告警概览与资源数量统计
监控	监控中心（监控对象统一管理）+十二类监控分类

菜单域	功能说明
告警	告警规则、告警中心（全生命周期管理）、通知策略（接收人/通知模板/通知渠道）
安全运营	安全驾驶舱、服务器审计（SSH 基座监测）、数据库审计（JDBC 核心资产审计）、任务运行安全透视、高危操作实时阻断
数据库备份	备份源、备份策略、备份记录、恢复任务
系统设置	系统参数、通用设置等平台基础配置管理

第四章 技术特性

4.1 架构特性

- **无 Agent（Agentless）**：无需在目标机器安装任何代理程序，多协议远程采集，部署与维护成本低
- **高度可扩展**：监控类型、采集协议、告警渠道、存储后端均以"抽象接口+可插拔实现"方式组织，插件化扩展
- **前后端分离**：Java 多模块后端+Angular 单页前端，功能裁剪层支持按客户场景定制交付形态
- **容器化部署**：微服务架构，各服务独立部署、故障自动拉起；安装部署约 20 分钟完成

4.2 信创适配

- 原生支持达梦数据库（dexp/dimp）、金仓数据库（sys_dump/sys_restore、sys_basebackup）备份恢复
- 支持信创环境部署（国产 CPU、国产操作系统、国产数据库）
- 纯 Java 技术栈，全栈国产化适配

4.3 可靠性设计

- 备份双副本存储、恢复二次确认、命令参数化执行、密码脱敏不入日志、执行超时控制
- 告警全生命周期留痕，安全事件处置全程可审计
- 监控指标实时入库，历史趋势可查，多时序数据库后端平滑切换

第五章 典型应用场景

应用场景	平台能力对应
数据安全合规	公共数据运营平台、数据中台等关键基础设施的统一监控与数据安全防护（数据库防火墙+审计+基础设施监测+驾驶舱）
数据容灾备份	关键配置数据的定时备份、异地容灾与快速恢复（内置备份恢复模块+双副本留存+时间点还原）
基础设施运维	主机、中间件、数据库、微服务的统一监控与告警（Agentless 多协议采集+智能告警中心）
数据库安全审计	数据库高危操作审计、SQL 注入检测与会话阻断（JDBC 原生审计+防火墙 Kill）

第六章 服务保障

- **技术支持**：7×24 小时技术支持（电话/邮件/远程协助），支持邮箱 support@oceandatum.com
- **常态化运维**：定期巡检、性能优化、安全漏洞修复、版本升级、备份恢复协助
- **培训服务**：分层培训（系统管理员/技术人员/业务人员），考核发证
- **补丁与版本**：安全补丁及时推送；补丁实行发布→灰度验证→通知→正式发放流程，保留回滚方案
- **远程演示**：提供远程演示环境（www.ottomi.cn），可远程操作验证产品功能

第七章 结语

Ottomi-Ops 3.0 智能运维平台深度融合监控告警、数据安全监测与备份恢复能力，为客户提供一套集"实时监控、智能告警、安全审计、容灾备份"于一体的综合运维解决方案。平台技术架构清晰、扩展性强，能够有效支撑关键数据基础设施的安全稳定运行。

第八章 联系我们

上海奥腾计算机科技有限公司

- 官网：www.oceandatum.com
- 咨询邮箱：info@oceandatum.com